REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-19 are currently pending in the present application, Claims 1, 7, 13, and 14 having been amended. Support for the amendments to Claims 1, 7, 13, and 14 is found, for example, in the originally filed specification at page 9, lines 25-33, page 14, line 30 to page 15, line 12, and page 19, lines 6-14. Applicants respectfully submit that no new matter is added.

In the outstanding Office Action, Claims 1, 2, 4-8, 10-15, and 17-19 were rejected under 35 U.S.C. §103(a) as unpatentable over Eliott (U.S. Patent No. 6,468,160); and Claims 3, 9, and 16 were rejected under 35 U.S.C. §103(a) as unpatentable over Eliott in view of Chan (U.S. Patent No. 6,473,860).

With respect to the rejection of Claim 1 as unpatentable over Eliott, Applicants respectfully submit that the amendment to Claim 1 overcomes this ground of rejection. Amended Claim 1 recites

> A program distribution device for distributing executable programs through a network to a client device having a tamper resistant processor which is provided with a unique secret key and a unique public key corresponding to the unique secret key in advance, the program distribution device comprising:
>
> a first communication path set up unit configured to set up a first communication path between the program distribution device and the client device for communications other than transfer of the executable programs;
>
> a second communication path set up unit configured to set up a second communication path directly connecting the program distribution device and the tamper resistant processor within the client device and dedicated for transfer of the executable programs such that the executable programs are not accessible by any other parts of the client device, the first and second communication paths being set up as different channels

> on an identical transmission line or as different transmission lines;
>
> an encryption processing unit configured to produce an encrypted program by encrypting an executable program to be distributed to the client device and executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor which is not shared with any other parts of the client device; and
>
> a transmission unit configured to transmit the encrypted program to the tamper resistant processor through the second communication path so that the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key.

As further clarified by the present amendment, the claimed invention is specifically directed to the case of using two separate communication paths of different types, namely the first and second communication paths that are set up as different channels on an identical transmission line or as different transmission lines, where the first transmission path is used for communications other than transfer of the executable programs and the second transmission path is used for transfer of the executable programs.[1]

The first communication path is an ordinary communication path between the program distribution device (server) and the client device, but the second communication path is a dedicated special communication path that directly connects the program distribution device (server) and the tamper resistant processor within the client device.

In this regard, the outstanding Office Action erroneously contends, in section 4 of the Office Action, that the above-noted features of Claim 1 are disclosed in col. 10, lines 57-67 and col. 27, lines 20-35 of Eliott.

However, col. 10, lines 57-67 of Eliott only describes a communication for authentication between a processor within a peripheral interface 138 which is a component of

[1] For example, see page 9, lines 25-33 of the present specification.

a video game console 52 and a security processor 152 within a storage device (game cartridge) 54.[2] When Eliott is properly interpreted, the server 101 shown in Fig. 11 of Eliott corresponds to the claimed program distribution device (server) for distributing programs through a network and the video game console 52 shown in Fig. 2 corresponds to the claimed client device that includes a processor for actually executing the distributed program (video game). It should be apparent that what is described in col. 10, lines 57-67 of Eliott is neither a first communication path between the program distribution device (server) and the client device (video game console), nor a second communication path between the program distribution device (server) and a processor within the client device (video game console) which actually executes the distributed program (video game).

Similarly, col. 27, lines 20-35 of Eliott only describes a communication between the server 101 and a disk controller associated with a hard drive 206 which is a component of an expansion device 95.[3] Again, when Eliott is properly interpreted, the server 101 shown in Fig. 11 of Eliot corresponds to the claimed program distribution device (server) for distributing programs through a network and the video game console 52 shown in Fig. 2 of Eliot corresponds to the claimed client device that includes a processor for actually executing the distributed program (video game). It is apparent that what is described in col. 27, lines 20-35 of Eliott is neither a first communication path between the program distribution device (server) and the client device (video game console), nor a second communication path between the program distribution device (server) and a processor within the client device (video game console) which actually executes the distributed program (video game). Even if the expansion device 95 of Eliott is interpreted as a part of the client device, the disk controller of the expansion device 95 of Eliott is clearly not a processor which actually executes the distributed program (video game), and the video game stored in the hard drive

[2] Eliott, Fig. 2.
[3] Eliott, Fig. 11.

206 is clearly accessible from the other parts of the client device such as a processor within the video game console 52 which actually executes the video game.

Thus, Eliott does not disclose or suggest anything corresponding to the claimed first and second communication paths.

The outstanding Office Action also contends that the above-noted features of Claim 1 are disclosed in col. 26, lines 37-62, and col. 27, lines 20-48 of Eliott. Applicants respectfully submit that this position is erroneous.

Col. 26, lines 37-62 of Eliott only describes exchanges of user name, password, authentication information, session information, etc., between the user's browser and the Internet service provider's server, without mentioning a communication path used for this purpose. Also, col. 27, lines 20-48 of Eliott only describes downloading of the control information from the server to the disk drive controller to securely control disk partitions that are created, and to control which applications have access to respective partitions. Although Eliott describes a direct security link between server 101 and a disk drive controller resident within the expansion device 95, this direct security link is to be realized by the Internet security features such as RSA's secure socket layer, firewalls, etc., so that it does not imply any specific feature of a communication path used for this purpose.

Applicants also point out that the disk drive controller is merely a digital signal processor associated with hard drive in the expansion device 95, and it is not a processor for executing programs (applications) in the video game system 50 which is the user's device, and it is not a tamper resistant processor. In this regard, in col. 25, lines 35-63 quoted on page 6 of the outstanding Office Action, Eliott only mentions a security check (or security authentication) between the security processor 180 and the security processor associated with the hard drive 206, but such a security check (security authentication) between processors has

absolutely nothing to do with a physical property of a processor itself. Thus, Eliott completely fails to disclose or suggest any processor that is tamper resistant.

Furthermore, Eliott fails to disclose any teaching for utilizing a dedicated special communication path that directly connects the program distribution device (server) and the tamper resistant processor within the client device, for the specific purpose of distributing executable programs to a type of the client device that has the tamper resistant processor provided inside.

Moreover, as also clarified in the present amendment to Claim 1, the claimed invention is specifically directed to the case of encrypting an executable program to be distributed to the client device and executed within the tamper resistant processor, by using the unique public key of the tamper resistant processor which is not shared with any other parts of the client device, and then sending the encrypted program from the program distribution device to the tamper resistant processor through the second communication path, so that the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key.[4]

In this regard, the outstanding Office Action contends that this feature is disclosed in col. 25, lines 18-28 and col. 29 lines 5-16 of Eliott. However, col., col. 25, lines 18-28 of Eliott only describes the encryption of the game software by the server 101 using the public key (private encryption key) transmitted to the server 101 from the DSP controller (hard drive controller) 194 associated with the hard drive 206, for the purpose of storing the game software in the hard drive 206 after processing by the video game system 50. Col. 29, lines 5-16, of Eliott only describes the encryption of the game software by the server 101 using the

[4] See, for example, the specification at page 14, line 30 to page 15, line 12.

encryption key unique to each individual hard drive 206 such as the unique ID and encryption keys for each expansion device 95. As already pointed out above, the hard disk controller 194 of the hard drive 206 of Eliott is clearly not a processor which actually executes the distributed program (video game), and the video game stored in the hard drive 206 is clearly accessible from the other parts of the client device such as a processor within the video game system 50 which actually executes the video game, which implies that the public key used in encrypting the game software is shared with the other parts of the client device such as a processor within the video game system 50. In particular, Eliott completely fails to describe any public key that is uniquely assigned to a processor which actually executes the video game or a use of such a public key for the purpose of encrypting a program to be delivered directly to a processor which actually executes the video game.

Thus, Eliott cannot be considered as disclosing the claimed encryption of the executable program by using a unique public key of the tamper resistant processor which is not shared with any other parts of the client device.

Section 8 of the outstanding Office Action takes the position that the above-noted features of the claimed invention are disclosed in col. 25, lines 15-40, col. 26, lines 18-37, col. 25, lines 14-24 and 29-63, and col. 29 lines 5-17 of Eliott. Applicants respectfully traverse this position.

Col. 25, lines 15-40, 14-24 and 29-63 of Eliott only describes the encryption of the game software by the server 101 using the private encryption key transmitted to the server 101 in encrypted form. Also, col. 26, lines 18-37 of Eliott only describes the encryption of the video games resident on hard drive 206 by the server using the unique ID as a key. Also, col. 29, lines 5-17 of Eliott only describes the encryption of the game software by the server 101 using the encryption key unique to each individual hard drive 206. As already pointed out above, the hard disk controller 194 of the hard drive 206 of Eliott is clearly not a processor

which actually executes the distributed program (video game), and the video game stored in the hard drive 206 is clearly accessible from the other parts of the client device such as a processor within the video game system 50 which actually executes the video game, which implies that the public key used in encrypting the game software is shared with the other parts of the client device such as a processor within the video game system 50. In particular, Eliott completely fails to describe any public key that is uniquely assigned to a processor which actually executes the video game or a use of such a public key for the purpose of encrypting a program to be delivered directly to a processor which actually executes the video game.

Thus, Eliott clearly fails to disclose any teaching for encrypting an executable program by using the unique public key of the tamper resistant processor such that the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key. Applicants note that these two features are combined in the claimed invention in a specific way to realize a specific technical effect, so that separate showing of each one of these features cannot obviate the claimed invention. Namely, a combination of the feature of encrypting the program by using the public key of the tamper resistant processor and the feature of transmitting the encrypted program through the second communication path of a type as discussed above has the significant technical effect of ensuring that the encrypted program is directly delivered to the tamper resistant processor and the encrypted program can be decrypted and executed only within the tamper resistant processor which is an only entity that has the unique secret key corresponding to the unique public key.[5] Eliott completely fails to disclose any teaching for such a specific combination of these features for the purpose of realizing such a technical effect.

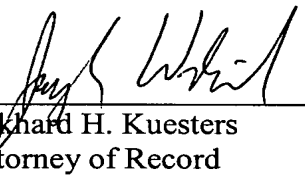
[5] For example, see page 19, lines 6-14 of the present specification.

Thus, Applicants respectfully submit that independent Claim 1 (and any claims dependent thereon) patentably distinguish over Eliott. Claims 7, 13, and 14 recite elements similar to those of Claim 1. Thus, Applicants respectfully submit that Claims 7, 13, and 14 (and any claims dependent thereon) patentably distinguish over Eliott, for at least the reasons stated for Claim 1.

Consequently, in view of the above amendments and comments, it is respectfully submitted that the outstanding rejection is overcome and the pending claims are in condition for allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Joseph Wrkich
Registration No. 53,796

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

I:\ATTY\JW\203058US\203058US_AM DUE 5-2-07.DOC